

Hinweise des Ministeriums des Innern vom 14. Oktober 2009 zur Verordnung zum Verfahrensverzeichnis (VerfVerzV) vom 10. September 2009 (GVBl. II S. 649)

In der oben genannten Verordnung hat die Landesregierung auf der Grundlage von § 8 Absatz 6 BbgDSG Regelungen bezüglich der Erstellung von Verzeichnissen über die bei der automatisierten Verarbeitung personenbezogener Daten angewendeten Verfahren getroffen. Nachfolgend werden diese Regelungen erläutert und Hinweise zum Ausfüllen des Musterformblattes für das Verfahrensverzeichnis gegeben. Hierbei werden nur die Punkte erläutert, die nicht selbsterklärend sind.

1 Erläuterung der Verordnung zum Verfahrensverzeichnis

§ 1 Absatz 1 VerfVerzV entspricht sinngemäß dem § 1 Absatz 1 der Verordnung zum Verfahrens- und Anlagenverzeichnis vom 23. November 1999 (GVBl. II S. 646). Das Musterformblatt zum Verfahrensverzeichnis wurde an die Änderungen der §§ 8 und 10 BbgDSG angepasst. Hinweise zum Ausfüllen des Musterformblattes werden unter Nummer 2 gegeben.

Zweck des Verfahrensverzeichnisses ist es, in komprimierter Form eine Übersicht über die einem konkreten Verfahren zugrundeliegenden, aus datenschutzrechtlicher Sicht wesentlichen Gesichtspunkte zu erhalten. Diese Übersicht dient zum einen der Selbstkontrolle der Daten verarbeitenden Stelle und zum anderen im Wege der Einsichtnahme in das Verzeichnis konkreter Verfahren der Transparenz der Datenverarbeitung für Betroffene.

Wie bisher ist das Verfahrensverzeichnis unverzüglich nach Beginn der jeweiligen automatisierten Verarbeitung personenbezogener Daten zu erstellen. Die hierfür im Wesentlichen erforderlichen Angaben sind aus dem Sicherheitskonzept nach § 7 Absatz 3 BbgDSG zu entnehmen.

§ 1 Absatz 2 enthält Regelungen für den Fall, dass mehrere öffentliche Stellen Verfahren zur automatisierten Verarbeitung personenbezogener Daten gemeinsam und/oder zentral betreiben oder betreiben lassen. Die für den zentralen Betrieb verantwortliche Stelle hat für die zentral betriebenen Komponenten oder Teilverfahren das Verfahrensverzeichnis zu fertigen und den das Verfahren nutzenden Stellen zur Verfügung zu stellen. Eine entsprechende Verpflichtung enthält § 2 Satz 2. Dies wird vor allem die Angaben zu den Nummern 9 und 11 (bezogen auf zentral bereit gestellte beziehungsweise genutzte Komponenten) betreffen. Die das Verfahren nutzenden Stellen haben, entsprechend ihrer Verantwortung für die materielle Rechtmäßigkeit des Verfahrens sowie für die Maßnahme nach § 10 BbgDSG, für ihren Bereich die Angaben für das Verfahrensverzeichnis festzulegen. Dies wird in der Regel die verbleibenden Punkte sowie die auf die dezentralen Komponenten bezogenen Angaben zu den Nummern 9 und 11 des Verfahrensverzeichnisses betreffen.

§ 1 Absatz 3 definiert, was unter einem neuen Verfahren oder einer wesentlichen Änderung eines bestehenden Verfahrens zu verstehen ist.

§ 1 Absatz 4 VerfVerzV enthält die Klarstellung, dass ein Verfahrensverzeichnis auch elektronisch geführt werden kann und dient der Verwaltungsvereinfachung, sofern die Daten verarbeitenden Stellen hiervon Gebrauch machen.

§ 2 Satz 1 VerfVerzV stellt klar, dass in den Fällen, in denen die zuständigen obersten Landesbehörden oder die von ihr bestimmte Stelle Verfahren auf der Grundlage von § 7 Absatz 3 Satz 5 BbgDSG freigeben, diese den Daten verarbeitenden Stellen die notwendigen Angaben für das Verfahrensverzeichnis zur Verfügung zu stellen haben.

Das heißt, den Daten verarbeitenden Stellen werden die Informationen beziehungsweise Festlegungen zur Verfügung gestellt, die durch die freigebende Stelle vorgegeben sind. Dies wird vor allem die Angaben zu den Nummern 3 bis 8 und 11 sowie gegebenenfalls der Nummer 9 betreffen. Lediglich dort, wo eigene Spielräume zur Verfahrensgestaltung bestehen, können und müssen die Daten verarbeitenden Stellen eigene Festlegungen treffen.

Eine entsprechende Verpflichtung zur Übermittlung regelt § 2 Satz 2 VerfVerzV bei von mehreren öffentlichen Stellen gemeinsam oder zentral betriebenen Verfahren für die Angaben bezüglich der zentral betriebenen Komponenten beziehungsweise Teilverfahren.

Durch § 3 Absatz 1 VerfVerzV wird klargestellt, dass die Einsichtnahme auch durch eine Veröffentlichung des Verfahrensverzeichnisses im Internet gewährleistet werden kann. Hierdurch können sich die anwendenden Stellen von Verwaltungsaufwand im Falle eines Einsichtsbegehrens entlasten. Nach einem Hinweis der LDA sind die Angaben zu § 8 Absatz 1 Nummer 8 und 9 BbgDSG nicht im Internet zu veröffentlichen, weil hierdurch potenzielle Angreifer Rückschlüsse auf möglicherweise vorhandene Sicherheitslücken ziehen könnten.

Nach § 3 Absatz 2 VerfVerzV muss die Daten verarbeitende Stelle die Gründe aufzeichnen, warum eine Einsichtnahme in die Angaben nach § 8 Absatz 1 Nummer 7 bis 11 BbgDSG die Sicherheit des Verfahrens beeinträchtigen würde. Hierdurch wird die ohnehin zu treffende Entscheidung über eine etwaige Nichtveröffentlichung nachvollziehbar dokumentiert. Es bedarf nicht bei jedem Einsichtsbegehren der erneuten Prüfung und gegebenenfalls Begründung der Entscheidung.

§ 4 VerfVerzV regelt das Inkrafttreten der Verordnung. Für neue Verfahren, die nach Inkrafttreten der VerfVerzV eingesetzt werden, ist ein Verfahrensverzeichnis auf der Grundlage der geänderten Verordnung zu erstellen. Eine Anpassung von Verzeichnissen zu bestehenden Verfahren muss erst bei einer wesentlichen Änderung des jeweiligen Verfahrens vorgenommen werden. Es wird jedoch empfohlen, eine Anpassung innerhalb von zwei Jahren nach Inkrafttreten der Verordnung vorzunehmen.

2 Ausfüllhinweise für das Musterformblatt

2.1 Vorbemerkung

Jede Stelle, die personenbezogene Daten selbst automatisiert verarbeitet oder im Auftrag verarbeiten lässt, hat für das dabei jeweils angewandte Verfahren die zugrunde liegenden wesentlichen datenschutzrechtlichen Aspekte in einem Verzeichnis darzustellen beziehungsweise festzulegen. Der Inhalt des Verzeichnisses ist in § 8 Absatz 1 BbgDSG geregelt. Der entsprechende Vordruck ist Anlage der Verfahrensverzeichnisverordnung und damit verbindlich vorgeschrieben.

Gemäß § 8 Absatz 5 BbgDSG ist die Erstellung eines Verfahrenszeichnisses zum Beispiel nicht erforderlich für Verfahren, deren einziger Zweck das Führen eines Registers ist, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse geltend machen können, zur Einsichtnahme offen steht. Auch für Verfahren, mit denen Datensammlungen erstellt werden, die nicht länger als drei Monate vorgehalten werden, Registraturverfahren oder Verfahren, die unter Einsatz handelsüblicher Schreibprogramme ablaufen, muss kein Verzeichnis erstellt werden. Letzteres gilt jedoch nur dann, wenn über übliche Suchbefehle hinaus eine personenbezogene Auswertbarkeit nach bestimmten Kriterien (zum Beispiel durch entsprechende Auswertprogramme) nicht gegeben ist. So ist beispielsweise für eine Verarbeitung personenbezogener Daten unter Nutzung von Tabellenkalkulationsprogrammen in der Regel ein Verfahrensverzeichnis zu erstellen.

Das Verfahrensverzeichnis muss unter anderem eine allgemeine Beschreibung der eingesetzten Datenverarbeitungsanlagen und der verwendeten Software enthalten.

Besonderes Gewicht ist auf die Darstellung der technischen und organisatorischen Maßnahmen nach § 10 BbgDSG zu legen. § 10 BbgDSG wurde im Zuge der Novellierung des Datenschutzgesetzes im Jahr 2007 neu gefasst. Die Änderungen sind bei der Erstellung des Verfahrenszeichnisses zu berücksichtigen. Die aufzuführenden Maßnahmen ergeben sich aus dem nach § 7 Absatz 3 Nummer 1 BbgDSG zu entwickelnden Sicherheitskonzept.

Soweit Verfahren zentral betrieben und von mehreren Daten verarbeitenden Stellen eingesetzt werden, wird für die zentral bereit gestellten Komponenten ein Verfahrensverzeichnis durch die für den zentralen Betrieb zuständige öffentliche Stelle geführt. Dieses ist, sofern erforderlich, den jeweiligen das Verfahren anwendenden beziehungsweise nutzenden Stellen zur Verfügung zu stellen (§ 2 Satz 2 VerfVerzV). Die das Verfahren nutzenden Daten verarbeitenden Stellen haben für ihren Verantwortungsbereich ebenfalls ein Verfahrensverzeichnis zu erstellen. Gegebenenfalls besteht das Verfahrensverzeichnis aus zwei Teilen, die die zentralen und dezentralen Komponenten abbilden. Ergänzend wird auf die Ausführungen zu § 1 Absatz 2 VerfVerzV (siehe oben) hingewiesen.

2.2 Zu den Angaben im Einzelnen:

- Daten verarbeitende Stelle

Hier ist die jeweilige Daten verarbeitende Behörde oder Einrichtung zu nennen, zum Beispiel das Ministerium X oder die Gemeinde Y. Die für das Verfahren fachlich verantwortliche Organisationseinheit innerhalb der öffentlichen Stelle wird unter Nummer 2 benannt.

- Regelungen zur Einsichtnahme

Bei der Erstellung des Verfahrenszeichnisses ist auf der Grundlage von § 8 Absatz 4 BbgDSG die Entscheidung zu treffen, ob es vollständig, teilweise oder gar nicht zur Einsichtnahme durch jedermann offen steht. Sofern eine Veröffentlichung im Internet erfolgt, dürfen die Angaben zu § 8 Absatz 1 Nummern 8 und 9 BbgDSG nicht zugänglich gemacht werden, weil anderenfalls potenzielle Angreifer Rückschlüsse auf möglicherweise vorhandene Sicherheitslücken ziehen könnten.

Gemäß § 3 Absatz 2 VerfVerzV sind die Gründe für eine Beschränkung der Einsichtnahme aufzuzeichnen. Diese sollten aus Zweckmäßigkeitsgründen dem Verfahrensverzeichnis als Anlage beigelegt werden. Eine Veröffentlichung der Gründe für eine Beschränkung der Einsichtnahme erfolgt nicht.

- Nummer 1 - Bezeichnung des Verfahrens

Die Bezeichnung sollte die Zweckbestimmung des Verfahrens erkennen lassen. Gleichzeitig ist festzuhalten, ob es sich um den erstmaligen Einsatz oder eine wesentliche Änderung des Verfahrens handelt. Wesentlich ist eine Änderung dann, wenn eine erneute Freigabe nach § 7 Absatz 3 zu erteilen ist. Dies ist insbesondere dann der Fall, wenn sich die den Angaben zu den Nummern 3 bis 7 sowie 9 und 10 zugrunde liegenden Sachverhalte nicht nur marginal verändert haben.

- Nummer 2 - Verantwortliche Organisationseinheit

Diese Angabe soll verdeutlichen, welche Organisationseinheit innerhalb einer Behörde die fachliche Verantwortung für das Verfahren trägt. Es ist die Stelle anzugeben, die für die materielle Rechtmäßigkeit der Datenverarbeitung verantwortlich ist. Diese muss innerhalb einer Behörde nicht mit der Stelle identisch sein, die die Freigabe für das Verfahren erklärt. Anzugeben ist dabei nicht die Ordnungsnummer beispielsweise eines Referates, sondern die Aufgabe, zum Beispiel Personalreferat, Jugendamt, Ausländerbehörde.

Durch diese Angabe ändert sich nichts an der datenschutzrechtlichen Verantwortung der Daten verarbeitenden Stelle.

- Nummer 3 - Zweckbestimmung und Rechtsgrundlage

Unter „3.1 - Zweckbestimmung“ sind alle Zwecke so konkret wie möglich zu nennen, zu denen die Verarbeitung personenbezogener Daten erfolgt. Begrenzt werden die zulässigen Zwecke durch die gesetzliche Aufgabenzuweisung beziehungsweise eine etwaige Einwilligungserklärung.

Unter „3.2 - Rechtsgrundlage“ ist die Ermächtigung für die Datenverarbeitung anzugeben.

Dabei ist die konkrete Rechtsnorm anzugeben, auf deren Grundlage die Verarbeitung personenbezogener Daten erfolgt. Ein allgemeiner Bezug zum Beispiel auf das SGB II reicht nicht aus. Es ist unter Angabe der zugrunde liegenden Rechtsnorm die spezifische Aufgabe zu benennen, der das Verfahren dient (zum Beispiel Bearbeitung von Anträgen auf Wohngeld nach dem Wohngeldgesetz, Bearbeitung von Anträgen auf Ausstellung eines Reisepasses).

- Nummer 4 - Betroffene Personengruppen und die diesbezüglichen Daten und Datenkategorien

Unter „4.1 - Kreis der Betroffenen“ sollen die Personen/-gruppen, deren Daten verarbeitet werden, so konkret wie möglich benannt werden, zum Beispiel „Personen, die einen Antrag auf ... gestellt haben“ oder „Kinder der Antragsteller“. Die Zahl der möglichen Betroffenen kann aufgrund von Erfahrungswerten geschätzt werden. Ist eine Schätzung nicht möglich, kann die Angabe unterbleiben.

Unter 4.2 ist die Art der gespeicherten Daten oder Datenkategorien anzugeben, zum Beispiel Personen-, Sach- oder Falldaten. Diese sind soweit wie möglich zu konkretisieren. Hierbei ist auch anzugeben, ob es sich dabei um die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 4a BbgDSG handelt. Sofern solche Daten verarbeitet werden sollen, ist an die Notwendigkeit der Vorabkontrolle gemäß § 10a BbgDSG zu denken.

- Nummer 5 - Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden

Unter Bezugnahme auf die Angaben zu Nummer 4 ist für jede Datenkategorie der Empfänger oder die Kategorien von Empfängern festzulegen. Dies betrifft die Empfänger, an die eine Mitteilung personenbezogener Daten bereits im Verfahren angelegt ist, also regelmäßig erfolgt.

Empfänger ist jede Person oder Stelle, die Daten erhält (§ 4 Absatz 4 Nummer 2 BbgDSG). Das heißt, hier sind auch Stellen innerhalb einer Behörde anzugeben, wenn diese personenbezogene Daten erhalten. Nicht anzugeben sind in dem Verfahrensverzeichnis Stellen, an die grundsätzlich keine Mitteilung vorgesehen ist, es aber dennoch auf Grund besonderer Fallkonstellation beziehungsweise auf der Grundlage spezieller Rechtsvorschriften zu einer Datenweitergabe kommen kann. Dies kann beispielsweise die Übermittlung an Polizeibehörden oder aber an Dritte, aufgrund eines rechtlichen Interesses des Dritten, betreffen, soweit die speziellen Voraussetzungen dafür vorliegen.

- Nummer 8 - Fristen für die Sperrung/Löschung der Daten (§ 19 BbgDSG)

Es ist festzulegen, innerhalb welcher Fristen regelmäßig eine Prüfung erfolgt, ob die Daten weiterhin zur Aufgabenerfüllung gemäß § 13 BbgDSG beziehungsweise der bereichsspezifischen Norm erforderlich sind oder eine Löschung oder Sperrung gemäß § 19 BbgDSG notwendig ist.

Sofern die der automatisierten Datenverarbeitung zugrunde liegende Rechtsvorschrift eine spezielle Löschungsvorschrift enthält, ist diese Frist unter Bezugnahme auf die Rechtsvorschrift als regelmäßige Lösungsfrist anzugeben.

- Nummer 9 - Kurzbeschreibung der technischen und organisatorischen Maßnahmen gemäß § 10 Absatz 2 BbgDSG

Die konkreten Maßnahmen ergeben sich aus dem Sicherheitskonzept nach § 7 Absatz 3 BbgDSG. Hier ist nur eine kurze Beschreibung vorzunehmen, die eine überschlägige Beurteilung der Angemessenheit der Maßnahmen in Bezug auf die mit dem Verfahren verbundenen Gefährdungen zulässt. Erläuternd wird hierzu auf die einzelnen Schutzziele der technischen und organisatorischen Maßnahmen hingewiesen:

- Gewährleistung von Vertraulichkeit

Vertraulichkeit ist dann gewährleistet, wenn die gespeicherten Daten nicht in die Hände Unbefugter geraten können. Dieses Ziel kann durch verschiedene Maßnahmen erreicht werden. In Betracht kommen die Festlegung von Modalitäten zur Benutzeridentifikation und -autorisierung. Dies kann durch die Vergabe von Benutzername und Passwort, aber auch durch die Nutzung von Chipkarten und PIN erfolgen. Des Weiteren ist ein Berechtigungskonzept notwendig, damit Nutzer nur auf die tatsächlich benötigten Daten zugreifen können. Zu denken ist auch an die sichere Aufbewahrung oder Unterbringung der verwendeten Hardware und Backup-Datenträger, die Nutzung von Verschlüsselungssoftware bei der Speicherung in unsicheren Umgebungen (zum Beispiel Notebook, Laptop, lokaler PC) oder besonders sensibler Daten in Datenbanken und bei der Datenübertragung in Netzwerken oder die vertrauliche Behandlung von Angaben über verwendete Hard- und Software und die Systemkonfiguration.

- Gewährleistung von Integrität

Integrität ist gewährleistet, wenn die Datenbestände unversehrt, vollständig und aktuell sind, also verlässlich richtig. Integrität muss während aller Phasen der Datenverarbeitung von der Erhebung bis zur Sperrung/Löschung gegeben sein (§ 3 Absatz 2 BbgDSG). Unter anderem muss gewährleistet sein, dass Daten nicht durch Computerviren oder andere Schadsoftware verfälscht werden.

- Gewährleistung von Verfügbarkeit

Verfügbarkeit bedeutet, dass die Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet oder genutzt werden können. Die Verfügbarkeit bezieht sich nicht nur auf die gespeicherten personenbezogenen Daten, sondern gleichermaßen auf die Hardware und die zur Verarbeitung erforderlichen Programme. Das Datenverarbeitungssystem ist hinsichtlich der Verfügbarkeit in seiner Gesamtheit zu betrachten.

- Gewährleistung von Authentizität

Die Authentizität ist dann gewährleistet, wenn ein Dokument beziehungsweise Datum zweifelsfrei seinem Ursprung zugeordnet werden kann.

Die Gewährleistung der Authentizität ist hauptsächlich bei elektronisch übertragenen Daten von Bedeutung. Den Gefährdungen kann durch Verfahren begegnet werden, bei denen die Herkunft der Daten nachvollziehbar ist. Bei der Bewertung der Verfahren sind verwendete Hardwarekomponenten und Programme einzubeziehen, zum Beispiel beim E-Government oder beim elektronischen Zahlungsverkehr. Beispiel: Einsatz von Signaturverfahren, bei denen rechtsverbindlich festgestellt werden kann, ob die Daten von den Betroffenen autorisiert (zum Beispiel digital signiert) worden sind oder wer der Urheber von Daten ist, die nicht von den Betroffenen stammen (zum Beispiel bei Datenübermittlung).

- Gewährleistung von Revisionsfähigkeit

Revisionsfähigkeit bedeutet, dass nachprüfbar ist, wie Daten in einen Datenbestand gelangt sind und welche Veränderungen sie im Laufe der Zeit durch wen erfahren haben. Nachprüfbar muss sein, wer für das Aufnehmen bestimmter Daten in einen Datenbestand oder ihr Entfernen daraus die Verantwortung trägt. Dies kann durch entsprechende Protokolldateien gewährleistet werden, die jedoch selbst ein datenschutzrechtliches Risiko bergen und deshalb einer engen Zweckbindung nach § 29 Absatz 4 BbgDSG unterliegen.

- Gewährleistung von Transparenz

Zur Herstellung von Transparenz sind automatisierte Verfahren in aktueller Form nachvollziehbar zu dokumentieren. Die einzelnen Verfahrensschritte müssen dabei so beschrieben werden, dass die Systematik der Prozesse ohne erheblichen zusätzlichen Aufwand nachvollziehbar wird. Transparenz wird vor allem durch die Dokumentation der Freigabe oder der Vorabkontrolle nach § 7 Absatz 3 BbgDSG, das ordnungsgemäße Führen des Verfahrensverzeichnis sowie der Dokumentation von wesentlichen Programmänderungen beziehungsweise die laufende Fortschreibung der Programmdokumentation hergestellt.

- Nummer 10 - Allgemeine Beschreibung der eingesetzten Datenverarbeitungsanlagen

Unter diesem Punkt sollen die zur Datenverarbeitung eingesetzten Anlagen und deren Zusammenwirken beschrieben werden. Des Weiteren ist die verwendete Software zu nennen. Die Angaben sind der Risikoanalyse beziehungsweise dem Sicherheitskonzept zu entnehmen.

- Nummer 11 - Freigabeerklärung

Gemäß § 7 Absatz 3 BbgDSG ist für jedes Verfahren, für das ein Verfahrensverzeichnis nach § 8 BbgDSG zu erstellen ist, die Freigabe zu erklären. Welche Organisationseinheit innerhalb einer Daten verarbeitenden Stelle die Freigabe erklärt, unterliegt der Organisationshoheit der jeweiligen Daten verarbeitenden Stelle. Dies muss nicht zwangsläufig die Organisationseinheit sein, die die fachliche Verantwortung für die (materielle) Rechtmäßigkeit des Verfahrens trägt. Aufgrund der Komplexität der nach § 10 BbgDSG zu treffenden technischen Maßnahmen kann die Freigabe - gegebenenfalls nach Bestätigung der materiellen Rechtmäßigkeit durch die fachlich zuständige Organisations-einheit - beispielsweise auch durch die für die Informationstechnik zuständige Organisationseinheit erfolgen. In jedem Fall ist die Fachebene in das Freigabeverfahren einzubeziehen.

Soweit Verfahren zentral betrieben und von mehreren Daten verarbeitenden Stellen eingesetzt werden, erfolgt eine Freigabe jeweils für den Verantwortungsbereich der einzelnen Daten verarbeitenden Stelle. Das heißt, für zentral betriebene Komponenten erfolgt eine Freigabe durch die hierfür verantwortliche Stelle; für dezentrale Komponenten erfolgt die Freigabe durch die jeweilige Daten verarbeitende Stelle auf dezentraler Ebene.

Vor der Freigabe kann gegebenenfalls das Votum des behördlichen Datenschutzbeauftragten eingeholt werden. Sofern Verfahren der Vorabkontrolle unterliegen, ist dieser ohnehin zu beteiligen.

Die Freigabeerklärung sowie das Ergebnis einer gegebenenfalls vorzunehmenden Vorabkontrolle sind dem Verfahrensverzeichnis als Anlage beizufügen.